

REMARKS

In response to the Final Office Action mailed July 17, 2001, Applicants respectfully request reconsideration.

Claims 1-32 have been examined. By this amendment, Applicants are amending claims 1, 2, and 15. As a result, claims 1-32 are pending with claims 1, 15, and 21 being independent claims. No new matter has been added.

Claim Rejections Under 35 U.S.C. §102(e)

Claims 1, 2, 5, 15-17, and 21-25 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,041,346 to Chen et al., (hereinafter Chen). In response, Applicants have made clarifying amendments to the claims and respectfully traverse the rejection as outlined below.

Chen is directed to a system for providing access to a remote network wherein an internet appliance, such as a router, is allowed to access a portion of a mass storage device (Abstract, Col. 2, line 26-38). Because internet appliances typically lack memory to perform applications such as electronic mail, Chen allocates a portion of an internal mass storage in another system on the network, such as a workstation or file server, and maps the mass storage in the other system to the internet appliance (Col. 3, lines 6-16, Col. 3, lines 57-65).

Figure 2 shows a flow chart describing an establishment of a link between the mass storage device and the internet appliance (Col. 4, lines 56-58). The mass storage device 180 is given a name in step 240 and users of the mass storage device 180 are then defined in step 250. For instance, mass storage device 180 may be a folder named virtual mailbox (Col. 5, lines 3-4). In step 250, internet appliance 110 is defined as a user, and a password required to access the mass storage device 180 is then provided via step 260 (Col. 5, lines 6-9). Because only identified users can access the mass storage device 180 and a password is required to be provided by the internet appliance 110 to access the mass storage device 180, the application residing in mass storage device 180 is secure (Col. 5, lines 9-13).

Figure 3 shows a method for accessing mass storage device 180 (Col. 5, lines 16-17). When the internet appliance 110, or another component of the network 100, attempts to access the mass storage device 180, then via step 310, the internet appliance 110 will search for the

component with the proper identity as defined in step 230 (Col. 5, lines 17-21). In step 320, the internet appliance 110 then finds the appropriate folder in the component using the name of the mass storage device 180 provided in step 240 (Col. 5, lines 21-24) [Emphasis added]. It is determined via step 330 whether the internet appliance 110 is a named user (Col. 5, lines 25-26). If the internet appliance is a named component, it must be determined if the password is correct, via step 340 (Col. 5, lines 28-30). If the correct password is not provided, access to the mass storage device 180 is denied, but if the password is correct, authorized users can access the mass storage device 180 (Col. 5, lines 30-34).

In summary, Chen discloses a device that accesses folders of another system using a user name and password to support an application that services users.

Claim 1 recites a data management method for managing access to a plurality of volumes of a storage system by at least two devices coupled to the storage system through a network. The method comprises steps of: (1) receiving over the network at the storage system a request from one of the at least two devices for access to at least one of the plurality of volumes of the storage system, the request identifying the at least one of the plurality of volumes in the storage system, and (2) selectively servicing, at the storage system, the request responsive to configuration data indicating that the one of the at least two devices is authorized to access the at least one of the plurality of volumes.

Chen does not anticipate claim 1. Chen teaches a technique whereby a device (i.e., the internet appliance) is provided access to an appropriate folder of a mass storage device by logging in using a user name and password combination (Col. 5, lines 21-34). By contrast, claim 1 recites a data management method for managing access to a plurality of volumes of a storage system. File folders are not volumes as alleged by the Examiner on Page 3, lines 5-6 of Paper No. 11. A volume, as is known in the art, is a logical grouping of disk storage devices that can be allocated to a device (e.g., a host) for storage space. Conversely, a folder is an organizational construct of a directory structure which is defined at a higher lever than a volume. Therefore, Chen does not disclose managing access to volumes of storage as claimed.

Further, Chen does not receive a request identifying at least one volume in a storage system. Rather, Chen obtains folders by indicating, to a mass storage device, a user name and password. Chen does not disclose a method wherein a request is received at a storage system

identifying a volume of the storage system to be accessed. Therefore, Chen does not anticipate the method recited in claim 1. Thus claim 1 is patentable over Chen, and the rejection should be withdrawn. Claims 2-14 depend from claim 1 and are patentable for at least the same reasons.

Claim 15

Independent claim 15 recites a computer readable medium comprising a first data structure to manage accesses by a plurality of devices to volumes of data at a storage system over a communication network, the storage system managing access responsive to a request identifying one of the plurality of volumes of the storage system to be accessed. The first data structure comprising a plurality of records corresponding to the plurality of devices, each of the plurality records corresponding to one of the plurality of devices and including configuration information having at least one identifier that identifies which of the volumes of the storage system the one of the plurality of devices is authorized to access.

Chen does not disclose the computer readable medium as recited in claim 15. In particular, Chen does not disclose a first data structure that manages accesses by a plurality of devices to "volumes of data" at a storage system as recited in claim 15. As discussed above, Chen teaches access control of a device to folders located on a system; not volumes of data. Further, as discussed above with respect to claim 1, Chen provides access to folders by indicating, to a mass storage device, a user name and password; Chen does not disclose a system that is responsive to a request identifying a volume of the storage system to be accessed. Therefore, claim 15 is patentable over Chen, and the rejection should be withdrawn. Claims 16-20 depend from claim 15 and are patentable for at least the same reasons.

Claim 21

Independent claim 21 recites a storage system comprising at least one storage device apportioned into a plurality of volumes, a configuration table to store centralized configuration data identifying which of a plurality of devices coupled to the storage system via a network are authorized to access each of the plurality of volumes, and a filter responsive to the configuration data, to selectively forward to the at least one storage device requests for access to the plurality of volumes received from the plurality of devices.

Chen does not disclose a storage system as recited in claim 21. Chen teaches a conventional file server that provides access to files and folders to an internet appliance; Chen does not teach or suggest a configuration table to store configuration data identifying which of a plurality of devices coupled to a storage system are authorized to access each of the plurality of volumes as recited in claim 21. As discussed above with respect to independent claim 1, Chen does not teach access to volumes; Chen teaches access to folders. Thus, the system of Chen does not disclose the storage system as recited in claim 21. Therefore, claim 21 is patentable over Chen, and the rejection should be withdrawn. Claims 22-31 depend from claim 21 and are patentable for at least the same reasons.

Attached hereto is a marked-up version of the changes made to the claims by the current amendment. The attached pages are captioned **“AMENDED CLAIMS SHOWING CHANGES.”**

CONCLUSION

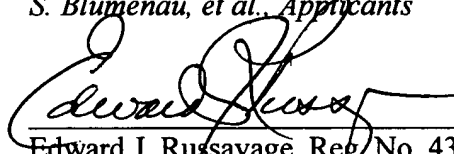
In view of the foregoing amendments and remarks, this application should now be in condition for allowance. A notice to this effect is respectfully requested. If the Examiner believed, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicants' attorney at the number listed below.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicants hereby request any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge the deficiency to Deposit Account No. 23/2825.

Respectfully submitted,

S. Blumenau, et al., Applicants

By:


Edward J. Russavage, Reg. No. 43,069
Richard F. Giunta, Reg. No. 36,149
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, Massachusetts 02210-2211
Tel. No.: (617) 720-3500
Attorney's for Applicants

Docket No. E0295/7066 (RFG/EJR)

Date: October 17, 2001

x10/17/01x

AMENDED CLAIMS SHOWING CHANGES

1. (Twice Amended) A data management method for managing access to a plurality of volumes of a storage system by at least two devices coupled to the storage system through a network, the method comprising steps of:

receiving over the network at the storage system a request from one of the at least two devices for access to [a portion of data stored at] at least one of the plurality of volumes of the storage system, the request identifying the at least one of the plurality of volumes in the storage system; and

selectively servicing, at the storage system, the request responsive to configuration data indicating that the one of the at least two devices is authorized to access [the portion of data] at least one of the plurality of volumes.

2. (Amended) The data management method according to claim 1, [where the storage system is arranged to store a plurality of volumes of data, and] wherein the configuration data is stored in the storage system in a configuration table comprising a plurality of records, each of the records including an identifier and information indicating which of the volumes of data are available to a device associated with the corresponding identifier, and wherein the step of selectively servicing further includes steps of:

receiving the request at the storage system issued by the one of the at least two devices, the request including a source identifier identifying the one of at the at least two devices that initiated the request and an address to one of the volumes of the plurality of volumes in the storage system; and

determining whether to service the request responsive to a portion of the configuration data associated with the source identifier and the address of the one of the volumes.

15. (Twice Amended) A computer readable medium comprising:

a first data structure to manage accesses by a plurality of devices to volumes of data at a storage system over a communication network, the storage system managing access responsive to a request identifying one of the plurality of volumes of the storage system to be accessed, the first data structure comprising a plurality of records corresponding to the plurality of devices, each of the plurality of records corresponding to one of the plurality of devices and including configuration information having at least one identifier that [identifying] identifies which of the volumes of the storage system the one of the plurality of devices is authorized to access.